CLAIMS

What is claimed is:

1. A method for establishing a secure communication session among a first node of a network and one or more other nodes using a group shared secret key, each of the nodes having a private key value associated therewith, the method comprising the computer-implemented steps of:

communicating a first public key value of the first node to a second node;

creating and storing an initial shared secret key for the first node and second node based on a first private key value and a second public key value that is received from the second node;

creating and storing information at the first node that associates the first node with a first network communication entity by generating a collective public key value that is shared by the first node and a second node and based on the first private key value and a second private key value that is derived by the first node from the second public key value;

receiving a third public key value from a third node that seeks to join the first network communication entity;

creating and storing a shared secret key value based on the collective public key value and the third public key value;

joining the first node to a second network communication entity that includes the first network communication entity and the third node and that uses secure communication with messages that are encrypted using the shared secret key value.

2. A method as recited in Claim 1, wherein joining the first node to a second network communication entity includes the step of communicating the first private key value to the second node and to the third node using messages encrypted using the shared secret key value.

3. A method as recited in Claim 1, wherein creating and storing a shared secret key value further comprises creating and storing the shared secret key based upon how many times each node of the second network communication entity has participated in formation of any such entity and based upon each private number of each node in the second network communication entity.

4. A method as recited in Claim 1, further comprising the step of creating and storing a subsequent shared secret key for use by the first network communication entity and the third node to enable the third node to independently compute the group shared secret key.

5. A method as recited in Claim 4, wherein creating and storing the subsequent shared secret key comprises creating and storing the subsequent shared secret key, k, according to the relation

$$k = p^{(a*x)(b*y)(c*z)} \bmod (q)$$

where p = a random number, q = a prime number, a = the first private key value, b = the second private key value, c = a private key value of the third node, x = a number of times the first node has participated in entity formation, y = a number of times the second node has participated in entity formation, and z = a number of times the third node has participated in entity formation.

6. A method as recited in Claim 5, further comprising the step of storing and distributing the first public value and the second public value using a key distribution center.

7. A method as recited in Claim 5, wherein the step of joining the first node to a second network communication entity further comprises:

creating and storing a collective public key based upon the first private key value, the second private key value, and the third private key value;

communicating a collective public key of the second network communication entity to the third node.

8. A method as recited in Claim 7, wherein the step of joining the first node to a second network communication entity further comprises determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based upon order of entry into the formed entity.

9. A method as recited in Claim 7, wherein the step of joining the first node to a second network communication entity further comprises determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based upon a predetermined metric.

10. A method as recited in Claim 1, wherein creating and storing an initial shared secret key for the first node and second node comprises creating and storing an initial shared public key "AB" according to the relation

$$AB = k_{ab}{}^{ab} \bmod (q) = p^{(ab)(ab)} \bmod (q)$$

wherein k = the initial shared secret key value, a = the first private key value, b = the second private key value, p is a base value, and q is a randomly generated prime number value.

11. A method for establishing a secure communication session among a first node of a network and one or more other nodes that are joined in a first network communication entity, using a group shared secret key, each of the nodes having a private key value associated therewith, the method comprising the computer-implemented steps of:

communicating a first public key value from a first node that is joining the first network communication entity to each other node that is currently within the first network communication entity;

receiving a collective public key value that is shared by each other node in the first network communication entity and that is based on private key values associated with each other node in the network communication entity;

creating and storing the group shared secret key value based on the collective public key value and the private key value associated with the first node;

joining the first node to a second network communication entity that includes the first network communication entity and the first node and that uses secure communication with messages that are encrypted using the shared secret key value.

12. A method as recited in Claim 11, wherein joining the first node to a second network communication entity includes the step of communicating the private key value of the first node to all other nodes that are in the first network communication entity using messages encrypted using the shared secret key value.

13. A method as recited in Claim 11, wherein creating and storing the group shared secret key value further comprises creating and storing the group shared secret key based upon how many times each node of the second network communication entity has participated in formation of any such entity and based upon each private number of each node in the second network communication entity.

14. A method as recited in Claim 11, further comprising the step of creating and storing a subsequent shared secret key for use by the

first network communication entity and the first node to enable the first node to independently compute the group shared secret key.

15. A method as recited in Claim 14, wherein creating and storing the subsequent shared secret key comprises creating and storing the subsequent shared secret key, k, according to the relation

$$k = p^{(a*x)(b*y)(c*z)} \bmod (q)$$

where p = a random number, q = a prime number, a = the first private key value, b = the second private key value, c = a private key value of the third node, x = a number of times the first node has participated in entity formation, y = a number of times the second node has participated in entity formation, and z = a number of times the third node has participated in entity formation.

16. A method as recited in Claim 11, further comprising the step of communicating the first public key value of the first node to the first network communication entity by storing the first public key value in a key distribution center.

17. A method as recited in Claim 11, wherein the step of joining the first node to a second network communication entity further comprises creating and storing a subsequent collective public key based upon the collective public key value and the first public key value of the first node.

18. A method as recited in Claim 11, wherein the step of joining the first node to a second network communication entity further comprises receiving the collective public key from one of the nodes of the first network communication entity that was the first node to join the first network communication entity.

19. A method as recited in Claim 11, wherein receiving the collective public key value comprises receiving an initial shared public key "AB" defined according to the relation

$$AB = k_{ab}{}^{ab} \bmod (q) = p^{(ab)(ab)} \bmod (q)$$

wherein k = the initial shared secret key value, a = the first private key value, b = the second private key value, p is a base value, and q is a randomly generated prime number value.

20. A method for exchanging cryptographic keys, the method comprising the steps of:

forming a multicast group initially comprising a first node and a second node, the first node generating a first private value, the second node generating a second private value, wherein the initial multicast group exchanges the first private value and the second private value with the second node and the first node, respectively, using a shared secret key, the multicast group generating a common public key; and

joining the multicast group by a new node, the new node generating a new private value and a corresponding public key, the step of joining includes:

sending the common public key of the multicast group by a member of the multicast group to the new node;

tracking a number of times each node in the multicast group participates in the step of joining;

computing a new shared secret key by the new node based upon the common public key of the multicast group and the new private value;

publishing the public key of the new node; and

computing the new shared secret key by each member of the multicast group based upon the public key of the new node, the private values of each member, and the number of times each node in the multicast group participates in the step of joining.

21. A method as recited in Claim 20, wherein the public values are stored and distributed by a key distribution center.

22. A method as recited in Claim 20, wherein the step of joining further comprises determining the sending member based upon order of entry into the multicast group.

23. A method as recited in Claim 20, wherein the step of joining further comprises determining the sending member based upon a predetermined metric.

24. A method as recited in Claim 20, wherein the plurality of nodes communicate over a packet switched network. that supports, in part, Internet Protocol.

25. A method as recited in Claim 20, wherein the first node, the second node, and the new node are authenticated by a distributed directory.

26. A computer-readable medium carrying one or more sequences of one or more instructions for establishing a secure communication session among a first node of a network and one or more other nodes using a group shared secret key, each of the nodes having a private key value associated therewith, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

communicating a first public key value of the first node to a second node;

creating and storing an initial shared secret key for the first node and second node based on a first private key value and a second public key value that is received from the second node;

creating and storing information at the first node that associates the first node with a first network communication entity by generating a collective public key value that is shared by the first node and a second node and based on the first private key value and a second private key value that is derived by the first node from the second public key value;

receiving a third public key value from a third node that seeks to join the first network communication entity;

creating and storing a shared secret key value based on the collective public key value and the third public key value;

joining the first node to a second network communication entity that includes the first network communication entity and the third node and that uses secure communication with messages that are encrypted using the shared secret key value.

27. A multicast communication server for establishing a secure communication session among a first node of a network and one or more other nodes using a group shared secret key, each of the nodes having a private key value associated therewith, comprising:

means for communicating a first public key value of the first node to a second node;

means for creating and storing an initial shared secret key for the first node and second node based on a first private key value and a second public key value that is received from the second node;

means for creating and storing information at the first node that associates the first node with a first network communication entity by generating a collective public key value that is shared by the first node and a second node and based on the first private key value and a second private key value that is derived by the first node from the second public key value;

means for receiving a third public key value from a third node that seeks to join the first network communication entity;

means for creating and storing a shared secret key value based on the collective public key value and the third public key value;

means for joining the first node to a second network communication entity that includes the first network communication entity and the third node and that uses secure communication with messages that are encrypted using the shared secret key value.

28. A method as recited in Claim 1, wherein creating and storing a shared secret key value further comprises creating and storing the shared secret key according to the relation

$k_{abc} = (AB)^c \bmod (q) = p^{(ab)(ab)c} \bmod (q) = p^{(ab**2)c} \bmod (q)$

where p = a random number, q = a prime number, a = the first private key value, b = the second private key value, c = a private key value of the third node, AB = the collective public key value.